แนวทางการดำเนินงานเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ต่อเว็บไซต์

1. การตรวจพบหรือรับทราบว่าเกิดเหตุภัยคุกคามทางไซเบอร์

1.1 กรณีส่วนงานหรือหน่วยงานเจ้าของเว็บไซต์ตรวจพบเองหรือรับทราบว่าเกิดเหตุภัยคุกคามทางไซเบอร์ ให้แจ้งเหตุภัยคุกคามทางไซเบอร์ พร้อมรายละเอียดที่เกี่ยวข้องไปยังสำนักเทคโนโลยีดิจิทัลและสารสนเทศ เพื่อดำเนินการตรวจสอบเหตุภัยคุกคามทางไซเบอร์เบื้องต้น

ช่องทางในการแจ้งเหตุภัยคุกคามทางไซเบอร์

- โทรศัพท์ : 02-727-3777, 02-727-3778 (ในวันและเวลาทำการ)
- Website : https://nida.ac.th/cyber-attack

1.2 กรณีสำนักเทคโนโลยีดิจิทัลและสารสนเทศตรวจพบเองหรือรับทราบว่าเกิดเหตุภัยคุกคามทางไซเบอร์ สำนักเทคโนโลยีดิจิทัลและสารสนเทศจะดำเนินการตรวจสอบเหตุภัยคุกคามทางไซเบอร์เบื้องต้น

2. สำนักเทคโนโลยีดิจิทัลและสารสนเทศ ดำเนินการตรวจสอบเหตุภัยคุกคามทางไซเบอร์เบื้องต้นและแจ้งผลการตรวจสอบ

2.1 สำนักเทคโนโลยีดิจิทัลและสารสนเทศดำเนินการตรวจสอบเหตุภัยคุกคามทางไซเบอร์เบื้องต้น ถึงสาเหตุภัยคุกคามทางไซเบอร์ ประเภทของภัยคุกคามทางไซเบอร์ ความเสียหายและผลกระทบที่เกิดขึ้นต่อเว็บไซต์แล้วแจ้งผลการตรวจสอบเบื้องต้นพร้อมทั้งแนวทางการแก้ไขทางโทรศัพท์หรืออีเมลไปยังส่วนงานหรือหน่วยงานเจ้าของเว็บไซต์

2.2 สำนักเทคโนโลยีดิจิทัลและสารสนเทศแจ้งผลการตรวจสอบเหตุภัยคุกคามทางไซเบอร์เป็นหนังสือส่งไปยังหน่วยงานเจ้าของเว็บไซต์

2.3 กรณีเป็นภัยคุกคามทางไซเบอร์ที่ละเมิดต่อข้อมูลส่วนบุคคล สำนักเทคโนโลยีดิจิทัลและสารสนเทศแจ้งผลการตรวจสอบเหตุภัยคุกคามทางไซเบอร์เป็นหนังสือส่งไปยังกองกฎหมายในฐานะ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ด้วย

3. การดำเนินการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์

3.1 สำนักเทคโนโลยีดิจิทัลและสารสนเทศดำเนินการตรวจสอบว่า เว็บไซต์ที่ถูกภัยคุกคามทางไซเบอร์นั้น อยู่ภายใต้การดูแลของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ หรือไม่

3.1.1 กรณีเป็นเว็บไซต์ที่อยู่ภายใต้การดูแลของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ สำนักเทคโนโลยีดิจิทัลและสารสนเทศจะดำเนินการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์

3.1.2 กรณีเป็นเว็บไซต์ที่ไม่ได้อยู่ภายใต้การดูแลของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ เช่น จ้างบุคคลภายนอกดูแล ไม่ได้ใช้ server ของสถาบันฯ ส่วนงานหรือหน่วยงานเจ้าของเว็บไซต์จะต้องดำเนินการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์

3.2 กรณีเป็นภัยคุกคามทางไซเบอร์ที่ละเมิดต่อข้อมูลส่วนบุคคล

ส่วนงานหรือหน่วยงานเจ้าของเว็บไซต์จะต้องบันทึกแบบแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลภายใน 24 ชั่วโมง นับแต่ทราบเหตุการละเมิดข้อมูลส่วนบุคคล (วันที่ได้รับแจ้งผลการตรวจสอบเป็นหนังสือจากสำนักเทคโนโลยีดิจิทัลและสารสนเทศ) โดยสามารถดาวน์โหลดแบบฟอร์มได้ที่ : https://nida.ac.th/cyber-attack

ช่องทางในการจัดส่งบันทึกแบบแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

- กองกฎหมาย
- อีเมล dpo-nida@nida.ac.th

หมายเหตุ

“**ข้อมูลส่วนบุคคล**” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“**การละเมิดข้อมูลส่วนบุคคล**” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

4. กองกฎหมายในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ดำเนินการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคล

กองกฎหมายในฐานะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะดำเนินการประเมินความเสี่ยงสำหรับการละเมิดข้อมูลส่วนบุคคลอันเกิดจากเหตุภัยคุกคามทางไซเบอร์ว่ามีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด โดยแบ่งเป็น 3 ระดับ ดังนี้

ระดับ 1 ไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล กองกฎหมายให้ข้อแนะนำเพื่อดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

ระดับ 2 มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล กองกฎหมายจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่สามารถกระทำได้

ระดับ 3 มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล กองกฎหมายจะต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่สามารถกระทำได้ และแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา

5. การแจ้งผลการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์

5.1 กรณีเป็นเว็บไซต์ที่อยู่ภายใต้การดูแลของสำนักเทคโนโลยีดิจิทัลและสารสนเทศสำนักเทคโนโลยีดิจิทัลและสารสนเทศจะแจ้งผลการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์เป็นหนังสือไปยังส่วนงานหรือหน่วยงานเจ้าของเว็บไซต์

5.2 กรณีเป็นเว็บไซต์ที่ไม่ได้อยู่ภายใต้การดูแลของสำนักเทคโนโลยีดิจิทัลและสารสนเทศ เช่น จ้างบุคคลภายนอกดูแล ไม่ได้ใช้ server ของสถาบันฯ ส่วนงานหรือหน่วยงานเจ้าของเว็บไซต์จะต้องแจ้งผลการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์เป็นหนังสือมายังสำนักเทคโนโลยีดิจิทัลและสารสนเทศ

5.3 สำนักเทคโนโลยีดิจิทัลและสารสนเทศจัดเก็บรวบรวมผลการดำเนินการแก้ไขและป้องกันเหตุภัยคุกคามทางไซเบอร์ด้านเทคนิคแล้วแจ้งเป็นหนังสือไปยังกองกฎหมายเฉพาะกรณีเป็นภัยคุกคามทางไซเบอร์ที่ละเมิดต่อข้อมูลส่วนบุคคล

5.4 กองกฎหมายเก็บรวมรวมและสรุปผลการดำเนินการเกี่ยวกับภัยคุกคามทางไซเบอร์ที่ละเมิดต่อข้อมูลส่วนบุคคล

ตัวอย่าง เหตุภัยคุกคามทางไซเบอร์กับเว็บไซต์

1. การ Hacked Website เช่น Gambling (การพนันออนไลน์) เพื่อแฝงหน้าเว็บพนันออนไลน์ในเว็บไซต์ของหน่วยงาน เพื่อเพิ่มโอกาสและประสิทธิภาพทางการค้นหา ผ่าน Search Engine

2. การโจมตีโดยเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ของหน่วยงานจากเดิมไปเป็นหน้าเว็บไซต์ใหม่ เพื่อทำลายความน่าเชื่อถือของหน่วยงาน

3. การสร้างหน้าเว็บปลอมเพื่อหลอก Phishing (ฟิชชิง) จุดประสงค์เพื่อข้อมูลสำคัญ เช่น การขอรหัสผ่าน หรือหมายเลขบัตรเครดิต และนำไปสู่การขโมยข้อมูลอื่น ๆ เป็นต้น